United Nations A/HRC/38/47

General Assembly

Distr.: General
18 June 2018

Original: English

Human Rights Council
Thirty-eighth session
18 June–6 July 2018
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the report of the Special Rapporteur on violence against women, its causes and consequences, prepared pursuant to Council resolution 32/19.

* The present report was submitted after the deadline in order to reflect recent developments.

GE.18-09877(E)
1809877

Please recycle

Contents

		Page
I.	Introduction	3
II.	Activities of the Special Rapporteur	3
III.	Online violence against women	4
	A. Introduction	4
	B. Definition, harm and manifestations of online and information and communications technology-facilitated violence against women and girls	6
	C. Application of the international human rights framework to online violence against women and girls	10
IV.	Conclusion and recommendations	18
	A. Recommendations for the United Nations	18
	B. Recommendations for States	19
	C. Recommendations for Internet intermediaries	21

I. Introduction

1. The present report is submitted pursuant to Human Rights Council resolution 32/19. In accordance with the mandate's priorities (see A/HRC/32/42), the Special Rapporteur on violence against women, its causes and consequences, Dubravka Šimonović, analyses online violence and violence facilitated by information and communications technology (ICT) against women and girls from a human rights perspective.

II. Activities of the Special Rapporteur

2. On 5 October 2017, the Special Rapporteur, pursuant to General Assembly resolution 69/147, presented her thematic report to the Assembly on the adequacy of the international legal framework on violence against women (A/72/134), in which she proposed the formulation of a global implementation plan on violence against women.

3. From 12 to 23 March 2018, the Special Rapporteur participated in the sixty-second session of the Commission on the Status of Women, held in New York, at which she delivered a statement,[1] and attended several high-level panel discussions on issues relating to violence against women. Within the context of the mandate's initiative on strengthening and institutionalizing cooperation between international and regional independent mechanisms on women's rights,[2] the Special Rapporteur organized consultations and high-level panel discussions on the themes "Institutional cooperation between global and regional independent mechanisms dealing with violence and discrimination against women" and "Fighting violence against women in politics" with the participation of the Deputy Secretary-General, the Director of the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), the Chair of the Committee on the Elimination of Discrimination against Women, two members of the Working Group on the issue of discrimination against women in law and in practice, the Chair of the African Commission on Human and Peoples' Rights, the President of the Inter-American Commission on Human Rights and the Rapporteur on the Rights of Women, the President of the Group of experts on action against violence against women and domestic violence of the Council of Europe and the President of the Committee of Experts of the Follow-up Mechanism to the Belém do Pará Convention.

4. The Special Rapporteur and other international and regional independent mechanisms on women's rights also held a meeting with the Secretary-General, who reiterated his support for the mandate's initiative on institutionalizing cooperation between independent international and regional mechanisms on violence against women.

5. On 4 November 2017, in Banjul, the Special Rapporteur participated in the sixty-first ordinary session of the African Commission on Human and Peoples' Rights, and delivered a statement[3] at the launch of its Guidelines on Combating Sexual Violence and its Consequences in Africa.

6. On 6 November 2017, in Washington D.C., the Special Rapporteur participated in an event convened by the Follow-up Mechanism to the Belém do Pará Convention on the theme "International and regional mechanisms on violence against women". On the following day, she attended a high-level event on "Regional and international Mechanisms for a comprehensive approach addressing violence against women and girls", with the participation of the Secretary-General of the Organization of American States.

---

[1] See www.ohchr.org/Documents/Issues/Women/SR/StatementCSW12March2018.pdf.

[2] See www.ohchr.org/EN/Issues/Women/SRWomen/Pages/CooperationGlobalRegionalMechanisms.aspx.

[3] Office of the United Nations High Commissioner for Human Rights (OHCHR), "Statement by Dubravka Simonovic, UN Special Rapporteur on violence against women at the 61st Ordinary Session of the African Commission on Human and Peoples' Rights", press release, 4 November 2017.

7. On 14 November 2017, in Geneva, the mandate holder attended the official launch by the Committee on the Elimination of Discrimination against Women of its general recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, in which the mandate holder actively participated upon invitation by the Committee.

8. On 22 November 2017, the Special Rapporteur, together with a group of independent human rights experts, marking the International Day on the Elimination of Violence against women, issued a call to eradicate gender-based violence against women, with a focus on sexual harassment and rape, urging States to update their national action plans in accordance with the new general recommendation adopted by the Committee on the Elimination of Discrimination against Women.[4] On 7 December, in order to mark the 16 Days of Activism against Gender-based Violence campaign and International Human Rights Day, the Special Rapporteur reiterated her call for the intensification of international, regional and national efforts to prevent femicide or gender-related killings of women, and for the worldwide adoption of a femicide watch or gender-related killings observatories.[5]

9. From 25 February to 2 March 2018, in Bogotá, Colombia, the Special Rapporteur attended the session of the Inter-American Commission on Human Rights, at which she delivered a statement during a hearing on sexual and reproductive rights of women and girls in Central America. From 14 to 18 May, the Special Rapporteur, pursuant to her mandate, participated in the twenty-seventh session of the Commission on Crime Prevention and Criminal Justice, and attended different panel discussions on gender-based violence against women and femicide.

10. The Special Rapporteur conducted a country visit to the Bahamas from 11 to 15 December 2017 (see A/HRC/38/47/Add.2; see also Add.1) and to Canada from 11 to 23 April 2018. During the period under review, the Special Rapporteur addressed, including jointly with other mandate holders, a total of over 50 communications relating to issues falling within the scope of her mandate. The Special Rapporteur also issued several press releases and statements jointly with other human rights mechanisms.

11. On 23 November 2017, in follow-up to a previous letter dated 4 April 2017, the Special Rapporteur addressed a letter to the Director of UN-Women as administrator of the United Nations Trust Fund in Support of Actions to Eliminate Violence against Women, to initiate cooperation with the Trust Fund, as envisaged by the General Assembly in its resolution 50/166.

III. Online violence against women[6]

A. Introduction

12. Online and ICT-facilitated forms of violence against women have become increasingly common, particularly with the use, every day and everywhere, of social media platforms and other technical applications (A/HRC/32/42 and Corr.1). In today's digital age, the Internet and ICT are rapidly creating new social digital spaces and transforming how individuals meet, communicate and interact, and by this more generally, reshape society as a whole. This development is especially critical for new generations of girls and

[4] OHCHR, "International Day on the Elimination of Violence against Women – 25 November", press release, 22 November 2017.

[5] OHCHR, "16 Days of Advocacy on ending violence against women and International Human Rights Day", press release, 7 December 2017.

[6] The present report was informed by inputs received from stakeholders pursuant to a call by the mandate holder for submissions, and a meeting, held on 16 and 17 January 2018, on due diligence to eliminate online violence against women, organized by the Due Diligence Project and the Association for Progressive Communications and hosted by the Global Women's Institute of the George Washington University.

boys, who are starting their lives extensively using new technologies to mediate in their relationships, affecting all aspects of their lives. In the section below, the Special Rapporteur considers the phenomenon of violence against women facilitated by new technologies and digital spaces from a human rights perspective.

13. Even though the core international human rights instruments, including those on women's rights, were drafted before the advent of ICT, they provide a global and dynamic set of rights and obligations with transformative potential, and have a key role to play in the promotion and protection of fundamental human rights, including a woman's rights to live a life free from violence, to freedom of expression, to privacy, to have access to information shared through ICT, and other rights.

14. When women and girls do have access to and use the Internet, they face online forms and manifestations of violence that are part of the continuum multiple, recurring and interrelated forms of gender-based violence against women. Despite the benefits and empowering potential of the Internet and ICT, women and girls across the world have increasingly voiced their concern at harmful, sexist, misogynistic and violent content and behaviour online. It is therefore important to acknowledge that the Internet is being used in a broader environment of widespread and systemic structural discrimination and gender-based violence against women and girls, which frame their access to and use of the Internet and other ICT. Emerging forms of ICT have facilitated new types of gender-based violence and gender inequality in access to technologies, which hinder women's and girls' full enjoyment of their human rights and their ability to achieve gender equality.[7]

15. Terminology in this area is still developing and not univocal. In several official United Nations documents, and in particular the 2030 Agenda for Sustainable Development, reference is made to the general and inclusive term "information and communications technology" (or ICT), while in other reports "online violence", "digital violence" or "cyberviolence" are used. In the present report, the Special Rapporteur refers to "ICT-facilitated violence against women" as the most inclusive term, but mainly uses "online violence against women" as a more user-friendly expression. Where appropriate, she uses both terms, as well as the terms "cyberviolence" and "technology-facilitated violence" as alternatives. Mindful that many forms of online violence covered in the report are perpetrated against both women and girls, she uses the term "women" in an inclusive manner, which includes girls whenever applicable,[8] while recognizing that girls are a frequent target of this form of violence.[9]

16. Despite being a relatively new phenomenon and, consequently, the lack of comprehensive data, it has been estimated that 23 per cent of women have reported having experienced online abuse or harassment at least once in their life, and that 1 in 10 women has experienced some form of online violence since the age of 15.[10]

17. At the normative level, the interaction between technology and women's human rights standards is marked by the recognition of the principle that human rights protected offline should also be protected online.[11] Since women's rights are human rights and the prohibition of gender-based violence has been recognized as a principle of international human rights law,[12] women's human rights as developed through comprehensive regional and international conventions, jurisprudence and norms should be protected online, including through the prohibition of gender-based violence in its ICT-facilitated and online

[7] See International Telecommunications Union (ITU), "ICT facts and figures 2016".

[8] Girls are also protected by legislation on child pornography, which is outside the scope of the present report.

[9] See the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the "Lanzarote Convention"). See also European Institute for Gender Equality, "Cyber violence against women and girls", 2017.

[10] See European Union Agency for Fundamental Rights, "Violence against women: an EU-wide survey", 2014.

[11] Human Rights Council resolution 32/13.

[12] Committee on the Elimination of Discrimination against Women general recommendation No. 35 (No. 19).

forms. Furthermore, States have established positive obligations to ensure that fundamental human rights are protected, respected and fulfilled.

18. Protecting women's human rights and eliminating violence against women and girls in public and private life in the "real world" remains a global challenge that has now spread to the digital space of social media, such as Instagram, Twitter, Facebook, Reddit, YouTube and Tumblr, and in other mobile telephone communications technology, micro-blogging sites and messaging applications (such as WhatsApp, Snapchat, Messenger, Weibo and Line), which are now a part of everyday life for many people around the world.

19. This new global digital space has great potential for ensuring the faster and fuller promotion and enjoyment of all human rights, including women's rights. The power to use this potential for protecting women's human rights and achieving gender equality does not, however, reside only in the technologies themselves; much also depends on the ways that people access and use those new technologies.[13] There is a significant risk that the use of ICT without a human rights-based approach and the prohibition of online gender-based violence could broaden sexual and gender-based discrimination and violence against women and girls in society even further.

20. Owing to the easy accessibility and dissemination of contents within in the digital world, the social, economic, cultural and political structures and related forms of gender discrimination and patriarchal patterns that result in gender-based violence offline are reproduced, and sometimes amplified and redefined, in ICT, while new forms of violence emerge. New forms of online violence are committed in a continuum and/or interaction between online or digital space: it is often difficult to distinguish the consequences of actions that are initiated in digital environments from offline realities, and vice versa. At this stage of development in ICT, it is essential that the different forms of online violence against women and girls be addressed through legislative and any other measures necessary to combat and prevent such violence, while upholding the right to freedom of expression, including access to information, the right to privacy and data protection, as well as the rights of women that are protected under the international human rights framework.

21. The aim of the present thematic report is to start the process of understanding how to effectively apply a human rights-based approach to prevent and combat online and ICT-facilitated violence against women as human rights violations, which shares its root causes with other forms of violence against women and should be dealt with in the broader context of the elimination of all forms of discrimination against women.

B. Definition, harm and manifestations of online and information and communications technology-facilitated violence against women and girls

1. Definition

22. Violence against women is a form of discrimination against women and a human rights violation falling under the Convention on the Elimination of All Forms of Discrimination and other international and regional instruments, according to which violence against women includes gender-based violence against women, that is, violence directed against a woman because she is a woman and/or that affects women disproportionately.[14] Article 1 of the Declaration on the Elimination of Violence against Women further specifies that violence against women is any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.

[13] See Thomas L. Friedman, "How Mark Zuckerberg Can Save Facebook – and Us", *New York Times*, 27 March 2018.

[14] Committee on the Elimination of Discrimination against Women general recommendations No. 19 (1992) on violence against women and No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19.

23. The definition of online violence against women therefore extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.

24. It is important to note from the outset that the Special Rapporteur report does not aim to define and catalogue all forms of online violence against women and girls. The rapid development of digital technology and spaces, including through artificial intelligence (AI), will inevitably give rise to different and new manifestations of online violence against women. She therefore aims to address some major concerns and to highlight some contemporary online forms of violence against women and girls brought to her attention. As digital spaces morph and develop, so too must the application and implementation of human rights norms to these areas. The Special Rapporteur considers online pornography and virtual manifestations of violence in video games, or violent interactive environments to be outside the scope of the present report.

2. Harm

25. The consequences of and harm caused by different manifestations of online violence are specifically gendered, given that women and girls suffer from particular stigma in the context of structural inequality, discrimination and patriarchy. Women subjected to online violence are often further victimized through harmful and negative gender stereotypes, which are prohibited by international human rights law. The Internet has become a site of diverse forms of violence against women and girls, in the form of pornography, sexist games and breaches of privacy. For women who engage in public debate through the Internet, the risk of harassment is experienced online; for example, an anonymous negative campaign calling for the gang rape of a woman human rights defender, with racist abuse posted in her Wikipedia profile. Female ICT users have publicly protested about sexist attacks (A/HRC/23/50, para. 66).

26. Acts of online violence may force women to retreat from the Internet. Research indicates that 28 per cent of women who had suffered ICT-based violence intentionally reduced their presence online.[15] Other common outcomes are social isolation, whereby victims or survivors withdraw from public life, including with family and friends, and limited mobility, when they lose their freedom to move around safely.

27. Online and ICT-facilitated acts of gender-based violence against women and girls include threats of such acts that result, or are likely to result, in psychological, physical, sexual or economic harm or suffering to women.[16] They can cause a high degree of psychological harm due to the scale and repeated occurrence of such acts. Victims and survivors experience depression, anxiety and fear, and in some cases may also develop suicidal tendencies. Technology-facilitated violence may also lead to physical harm (including suicides), as well as economic harm. In some instances, the threat of physical harm becomes a reality, when sexually explicit images or videos are posted on specialized advertising sites for prostitution together with private information, such as a victim's home address. Economic harm can be done when the explicit image of a victim of cyberabuse covers several pages of search engine results, making it difficult for the victim to find employment, or even preventing the victim from even attempting to find employment because of the shame and fear of potential employers discovering the images. Risk of harm arises from both online content (sexist, misogynistic, degrading and stereotyped portrayals of women, online pornography) and behaviours (bullying, stalking, harassment, intimidation facilitated and perpetrated via social media, tracking applications, and profiling technology).

[15] See Japleen Pasricha, "'Violence' Online in India: Cybercrimes Against Women & Minorities on Social Media", Feminism in India, 2016.

[16] See webpage of the Association for Progressive Communications on violence against women online at www.genderit.org/onlinevaw/countries.

28. Women are both disproportionately targeted by online violence and suffer disproportionately serious consequences as a result. Their access to technology is also affected by intersectional forms of discrimination based on a number of other factors, such as race, ethnicity, caste, sexual orientation, gender identity and expression, abilities, age, class, income, culture, religion, and urban or rural setting. These forms of discrimination are intersectional in that they are not only the result of a single particular individual characteristic but the result of the interplay between them, which can result in more severe consequences. Women who have multiple identities are often targeted online on the basis of a combination of these factors, including racial discrimination and hate speech. Some groups of women, such as women human rights defenders, women in politics, including parliamentarians,[17] journalists,[18] bloggers, [19] young women, women belonging to ethnic minorities and indigenous women,[20] lesbian, bisexual and transgender women,[21] women with disabilities and women from marginalized groups are particularly targeted by ICT-facilitated violence (see A/HRC/35/9).

29. Women human rights defenders, journalists and politicians are directly targeted, threatened, harassed or even killed for their work. They receive online threats, generally of a misogynistic nature, often sexualized and specifically gendered. The violent nature of these threats often leads to self-censorship. Some resort to the use of pseudonyms, while others maintain low online profiles, an approach that can have a detrimental impact on their professional lives and reputations. Others decide to suspend, deactivate or permanently delete their online accounts, or to leave the profession entirely. Ultimately, the online abuse against women journalists and women in the media are a direct attack on women's visibility and full participation in public life.[22] The anonymity of perpetrators further heightens the fear of violence, resulting in a sense of insecurity and distress experienced by the victims. In addition to the impact on individuals, a major consequence of online and ICT-facilitated gender-based violence is a society where women no longer feel safe either online or offline, given the widespread impunity for perpetrators of gender-based violence.[23] Online violence against women not only violates a woman's right to live free from violence and to participate online but also undermines democratic exercise and good governance, and as such creates a democratic deficit.

3. Manifestations

30. While many forms of online violence are not completely new, they take many forms and target women and girls in multiple and different ways by owing to the specificity of types of ICT, such as fast spreading ("viral") and global searchability, and the persistence, replicability and scalability of information, which also facilitates the contact of aggressors with the women they target, as well as secondary victimization. [24] Technology has transformed many forms of gender-based violence into something that can be perpetrated

---

[17] Inter-Parliamentary Union, "Sexism, harassment and violence against women parliamentarians", Issues Brief, October 2016.

[18] See Human Rights Council resolution 33/2, in which the Council condemned unequivocally the specific attacks on women journalists in the exercise of their work, including sexual and gender-based discrimination and violence, intimidation and harassment, online and offline.

[19] OSCE, *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists* (2016), p. 5.

[20] See Association for Progressive Communications, "Erotics: Sex, rights and the internet", 2011; Jane Bailey and Sara Shayan, "Missing and murdered indigenous women crisis: technological dimensions", *Canadian Journal of Women and the Law*, vol. 28, No. 2 (2016).

[21] Witness Media Lab, *Capturing Hate: Eyewitness Videos Provide New Source of Data on Prevalence of Transphobic Violence* (2016).

[22] See Office of the Representative on Freedom of the Media of the Organization for Security and Cooperation in Europe (OSCE), *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists* (OSCE, Vienna, 2016), and Committee to Protect Journalists, *Attacks on the Press*, 2016 Edition, Gender and Media Freedom Worldwide.

[23] See Internet Governance Forum, best practice forum on gender access, 2016.

[24] See Danah Boyd, "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications", in *Networked Self: Identity, Community and Culture on Social Network Sites* (Routledge, New York, 2011), pp. 39–58.

across distance, without physical contact and beyond borders through the use of anonymous profiles to amplify the harm to victims. All forms of online gender-based violence are used to control and attack women and to maintain and reinforce patriarchal norms, roles and structures and an unequal power relationship. This is particularly evident when violence, threats and harassment follow speeches or expression related to gender equality and feminism, or where defenders of women's rights are targeted for their work.

31. ICT may be used directly as a tool for making digital threats and inciting gender-based violence, including threats of physical and/or sexual violence, rape, killing, unwanted and harassing online communications, or even the encouragement of others to harm women physically. It may also involve the dissemination of reputation-harming lies, electronic sabotage in the form of spam and malignant viruses, impersonation of the victim online and the sending of abusive emails or spam, blog posts, tweets or other online communications in the victim's name. ICT-facilitated violence against women may also be committed in the work place[25] or in the form of so-called "honour-based" violence or of domestic violence by intimate partners. Women who speak out about their abuse online are frequently and increasingly threatened with legal proceedings, such as for defamation, which aims to prevent them from reporting their situation. Such behaviour may form part of a pattern of domestic violence and abuse.

32. ICT tools are also used for trafficking in women and girls, or as a threat to compel them into trafficking situations. Abusers may threaten the disclosure of private information online to maintain power and control over their victims to prevent them from leaving the relationship and/or from reporting abuse and pursuing their legal rights in court.

33. There are many new emerging forms of violence against women with ICT-related names, such as "doxing", "sextortion" and "trolling". Some forms of violence against women carry the prefix "online", such as online mobbing, online stalking and online harassment. New forms of violence have also developed, such as the non-consensual distribution of intimate contents ("revenge porn").

34. Online violence against women may be manifested in different forms and through different means, such as non-consensual accessing, using, manipulating, disseminating or sharing of private data, information and/or content, photographs and/or videos, including sexualized images, audio clips and/or video clips or Photoshopped images.

35. "Sextortion" refers to the use of ICT to blackmail a victim. In such cases, the perpetrator threatens to release intimate pictures of the victim in order to extort additional explicit photos, videos, sexual acts or sex from the victim.

36. "Doxing" refers to the publication of private information, such as contact details, on the Internet with malicious intent, usually with the insinuation that the victim is soliciting sex (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of exposing the woman to the "real" world for harassment and/or other purposes). It includes situations where personal information and data retrieved by a perpetrator is made public with malicious intent, clearly violating the right to privacy.

37. "Trolling" consists in the posting of messages, the uploading of images or videos and the creation of hashtags for the purpose of annoying, provoking or inciting violence against women and girls. Many "trolls" are anonymous and use false accounts to generate hate speech.[26]

38. Online mobbing and harassment refer to the online equivalents of mobbing or harassment on social platforms, the Internet, in chat rooms, instant messaging and mobile communications.

---

[25] See International Labour Office, "Ending violence and harassment against women and men in the world of work", International Labour Conference, 107th session, 2018.

[26] Instituto de las Mujeres del Distrito Federal, Programa Annual PAIMEF 2016: "CDMX Ciudad Segura y Amigable para las Mujeres y las Niñas", p. 20.

39. Online stalking is the repeated harassment of individuals, perpetrated by means of mobile phones or messaging applications, in the form of crank calls or private conversations on online applications (such as WhatsApp) or in online chat groups.[27]

40. Online sexual harassment refers to any form of online unwanted verbal or non-verbal conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular by creating an intimidating, hostile, degrading, humiliating or offensive environment.

41. "Revenge porn" consists in the non-consensual online dissemination of intimate images, obtained with or without consent, with the purpose of shaming, stigmatizing or harming the victim.

42. All the above-mentioned forms of online violence create a permanent digital record that can be distributed worldwide and cannot be easily deleted, which may result in further victimization of the victim. Relevant data and surveys have shown that, in the majority of cases, online violence is not a gender-neutral crime. Surveys of the gender dimension of online violence indeed indicate that 90 per cent of those victimized by non-consensual digital distribution of intimate images are women.[28]

C. Application of the international human rights framework to online violence against women and girls

1. Soft law developments addressing online violence against women and girls

43. In the past decade, there have been significant soft law developments in the understanding and recognition of online gender-based violence in the international human rights framework on women's rights and violence against women.

44. The issue of online gender-based violence was first addressed in 2006 by the Secretary-General in his in-depth study on all forms of violence against women (A/61/122/Add.1 and Corr.1), in which he noted that more inquiry about the use of ICT was needed so that emerging forms of violence could be recognized and better addressed.

45. In its resolution 20/8, the Human Rights Council clearly stated that the same rights that people have offline must also be protected online. The view of the Internet and digital technologies as enablers of rights and the digital space as an extension of rights held offline paved the way for discussions on how digital technologies had an impact on women's and girls' rights, specifically with regard to gender-based violence.[29]

46. In 2013, in its agreed conclusions, the Commission on the Status of Women called upon States to use ICT to empower women and to develop mechanisms to combat violence against women and girls (see E/2013/27).

47. In 2013, the General Assembly, in its resolution 68/181, went further by expressing its grave concern that women human rights defenders were at risk of and suffered from violations perpetrated both online and offline by State and non-State actors, and called upon States to exercise due diligence and to promptly bring perpetrators to justice.

48. In 2015, the Human Rights Council, in its resolution 29/14, recognized that domestic violence could include acts such as cyberbullying and cyberstalking — thereby reinforcing the framing of online gender-based violence as part of the continuum of violence against women — and that States had a primary responsibility for preventing and promoting the human rights of women and girls facing violence, including those facing domestic violence.

49. In 2016, the General Assembly, in its resolution 71/199, recognized that women were particularly affected by violations of the right to privacy in the digital age, and called

[27] See https://genderingsurveillance.internetdemocracy.in/.

[28] See the website of the Cyber Civil Rights Initiative at www.cybercivilrights.org.

[29] See Association for Progressive Communications and Hivos, "Global Information Society Watch 2013: Women's rights, gender and ICTs", 2013.

upon all States to further develop preventive measures and remedies. In 2017, the Human Rights Council, in its resolution 34/7, reaffirmed this call, noting that abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and persons in vulnerable situations, or marginalized groups.

2. International human rights law applicable to online violence against women and girls

(a) The right to live free from gender-based violence

50. International and regional human rights instruments set out States' obligations to combat all forms of discrimination against women, including online violence against women, and to protect their human rights, including every woman's right to be free from violence. The core women's human right instruments, such as the Convention on the Elimination of All Forms of Discrimination against Women, the Declaration on the Elimination of Violence against Women and the Beijing Declaration and Platform for Action, predate the development of the Internet and ICT, and consequently the emerging forms of online violence against women. The Convention on the Elimination of All Forms of Discrimination against Women has been progressively analysed by the Committee on the Elimination of Discrimination against Women, which has addressed ICT-facilitated violence against women in several general recommendations and concluding observations. In its general recommendation No. 33 (2015) on women's access to justice, it recognized the important role of digital spaces and ICT for women's empowerment. Furthermore, in its general recommendation No. 35 (2017) on gender-based violence against women, the Committee made clear that the Convention was fully applicable to technology-mediated environments, such as the Internet and digital spaces, as settings where contemporary forms of violence against women and girls were frequently committed in their redefined form. In addition, it highlighted the important role of ICT in transforming social and cultural stereotypes about women, as well as its potential in ensuring effectiveness and efficiency of women in their access to justice (see general recommendation No. 34 (2016) on the rights of rural women).[30] In its general recommendation No. 36 (2017) on the right of girls and women to education, the Committee also recognized how girls are affected by cyberbullying, particularly in relation to their right to education. Recognizing the potential that ICT and social media have to increase access to information and education, States should develop and implement educational programmes, including comprehensive women's human rights education.

51. At the regional level, in the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, the States members of the Council clearly request States to encourage the private sector, with due respect for freedom of expression, to participate in the implementation of policies aimed at preventing violence against women and to promote educational programmes for users on ways to address abusive online content of a sexual or violent nature.

(b) The right to live free from gender-based violence and the right to freedom of expression and access to information

52. Freedom of expression, enshrined in article 19 of the Universal Declaration on Human Rights and article 19 of the International Covenant on Civil and Political Rights, which guarantees the right of everyone "to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his/her choice", is now exercised in the digital space with the use of ICT and the Internet, including the right to seek, receive and impart information freely on the Internet without censorship or other interference. Freedom of expression is not, however, an absolute right, given that it cannot be invoked to justify language or other forms of expression designed to incite discrimination, hostility or violence (International Covenant on Civil and Political Rights, art. 20 (2)), including online violence against women. Legislation intended to protect

[30] See also Carly Nyst, "Technology-related violence against women: Recent legislative trends", Association for Progressive Communications, May 2014.

women against online violence but not carefully designed in accordance with the international human rights framework may have adverse collateral effects on other human rights; for instance, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression already pointed out that any State-imposed content restrictions should be provided by law, pursue one of the purposes set out in article 19, paragraph 3 of the Covenant, and respect the principles of necessity and proportionality (see A/HRC/17/27, para. 24 and A/66/290, para. 15).[31] In a joint statement with the mandate holder, the Special Rapporteur had previously stressed that online gender-based abuse and violence assaulted the basic principles of equality under international law and freedom of expression, and underlined that ensuring an Internet free from gender-based violence enhanced women's empowerment. They also highlighted the fact that women victims and survivors needed transparent and fast responses and effective remedies, which could only be achieved if both States and private actors worked together and exercised due diligence to eliminate online violence against women.[32]

53. Access to information includes access to ICT, which is often marked by gender inequality or a gender digital divide, namely, gender-based discrimination against women with regard to their access to and use of ICT, which hinders women's full enjoyment of their human rights. Women's access to ICT is part of their right to freedom of expression, and is necessary for the fulfilment of other basic human rights, such as the rights to participate in political decision-making and to non-discrimination.

54. According to the International Telecommunications Union (ITU), between 2013 and 2017, the proportion of women using the Internet was 12 per cent lower than the proportion of men using the Internet worldwide. In 2017, the global Internet penetration rate for men stood at 50.9 per cent, compared to 44.9 per cent for women. While the gender gap had narrowed in most regions since 2013, it had widened in Africa. In Africa, the proportion of women using the Internet was 25 per cent lower than the proportion of men. In least developed countries, only one out of seven women was using the Internet compared with one out of five men.[33]

55. In this regard, the 2030 Agenda for Sustainable Development recognizes that the spread of ICT and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies. Under Sustainable Development Goal 5, it sets the objectives of achieving gender equality and the empowerment of all women and girls through, among others, the elimination of all forms of violence against all women and girls in the public and private spheres (target 5.2) and of enhancing the use of enabling technology, in particular ICT, to promote women's empowerment (target 5.9). Moreover, Goal 9, target c urges States to significantly increase access to ICT and strive to provide universal and affordable access to the Internet in least developed countries by 2020. Similarly, the Committee on the Elimination of Discrimination against Women, in its general recommendation No. 34 (2016) on the rights of rural women, highlighted that ICT played a key role for the realization of women's human rights and that States had an obligation to improve and promote gender equality in the ICT sector.[34] At the regional level, article 17 of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa states that "women shall have the right to live in a positive cultural context and to participate at all levels in the determination of cultural policies".

56. In addition, in his report on ways to bridge the gender digital divide from a human rights perspective (A/HRC/35/9), the United Nations High Commissioner for Human Rights stressed that online violence against women must be dealt in the broader context of

[31] In this regard, see also the factsheet of the European Court of Human Rights on Hate Speech (March 2018), available at www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf.

[32] OHCHR. "UN experts urge States and companies to address online gender-based abuse but warn against censorship", press release, 8 March 2017.

[33] ITU, ICT Facts and Figures 2017 (available from www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf).

[34] See also Carly Nyst, "End violence: Women's rights and safety online, Technology-related violence against women: Recent legislative trends", Association for Progressive Communications, May 2014.

offline gender discrimination and violence, and that States should enact adequate legislative measures and ensure appropriate responses to address the phenomenon.

(c) The right to live free from gender-based violence and the right to privacy and data protection

57. The right to privacy, as recognized under article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, has been challenged in the digital environment. Data protection norms have also been challenged by ICT innovations that have increased the capacity of States and of non-State actors to conduct surveillance, decryption and mass data collection and use, which have an impact on the individual's rights to privacy. Many forms of online violence are per se acts of gender-based violence that violate women's and girls' rights to privacy; for example, the publication or posting online without consent of intimate photographs or Photoshopped images that are sexualized or have been created to humiliate, shame or stigmatize a woman is a violation of a woman's right to dignity and to live a life free from violence.

58. In a recent report, the Special Rapporteur on the right to privacy highlighted the need to examine cyberviolence against the more vulnerable, including domestic violence enabled by digital devices, risks to the privacy of young children and embedded gender and other biases in algorithms (A/HRC/37/62).

59. With the increasingly massive collection and storage of data by intermediaries and other corporations, the protection of privacy is crucial. In 2013, the General Assembly has expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights, as in the case of its resolution 68/167. Companies that collect and store massive amounts of data should, like data banks, bear the responsibility to protect their customers' personal data. The General Data Protection Regulation adopted by the European Union will, inter alia, require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure. It will also assert extraterritorial jurisdiction, given that it is applicable to all companies in the European Union as well as to international companies that collect or process personal data from subjects residing in it.

60. Encryption and anonymity, separately or together, create a zone of privacy to protect freedom of expression and to facilitate the freedom to seek, receive and impart information and ideas, regardless of frontiers. Anonymity online is an important role for women and others at risk of discrimination and stigma, in that it allows them to seek information, find solidarity and support and share opinions without fear of being identified. This holds particularly true for individuals who face discrimination and persecution based on their sexual orientation and gender identity (see A/HRC/29/32).

61. On related matters, a recent judgment by the Court of Justice of the European Union, commonly referred to as *Google v. Spain*,[35] established the "right to be forgotten" for victims, according to which individuals may request to be delisted from search results produced on the basis of a search term that includes their name when the data associated with their name is "inadequate, irrelevant or no longer relevant" for the purposes of data processing and if the information does not pertain to a public figure or is not of public interest.

3. States' human rights obligations to prevent and combat online violence against women and girls

62. States have a human rights obligation to ensure that both State and non-State agents refrain from engaging in any act of discrimination or violence against women. States have a direct responsibility concerning violence perpetrated by agents of the State itself. They also have due diligence obligations to prevent, investigate and punish acts of violence against women committed by private companies, such as Internet intermediaries, in accordance with article 2 (e) of the Convention on the Elimination of All Forms of Discrimination

[35] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

against Women. According to article 4 (c) of the Declaration on the Elimination of Violence against Women, States should exercise due diligence to prevent, investigate and punish acts of violence against women.

63. Under its general recommendation No. 35 (2017), the Committee on the Elimination of Discrimination against Women recommended that States encourage the private sector, including businesses and transnational corporations, to take all appropriate measures to eliminate all forms of discrimination, including violence against women, and to take responsibility for any forms of violence. It follows that online and social media should be encouraged to create or strengthen mechanisms focusing on the eradication of gender stereotypes, and to end any gender-based violence committed on their platforms.

64. The fact that violations are perpetrated beyond the territorial limits and jurisdiction of States also make it difficult for authorities, including law enforcement agencies, to identify, investigate, prosecute perpetrators and provide remedies for survivors of gender-based violence. It may also require extraterritorial cooperation between States.[36]

65. More specifically, States obligations concern a number of key areas, as described below.[37]

(a) Prevention

66. Prevention includes measures to provide awareness of ICT-facilitated violence against women and girls as forms of violence against women, as well as to establish and provide information on services and legal protection available to stop violations and to prevent their reoccurrence. States have an obligation to take all steps necessary to prevent human rights violations perpetrated abroad by Internet intermediaries over which they exercise influence, whether by regulatory means or by the use of incentives.[38]

(b) Protection

67. The obligation to protect victims of online violence against women encompasses the establishment of procedures for the immediate removal of gender-based harmful content through the elimination of the original material or its distribution. Protection also requires immediate judicial action in the form of national court orders and the prompt intervention of Internet intermediaries and, occasionally, may also require extraterritorial cooperation.[39] It includes the provision of accessible services for survivors, such as legal aid services. Protection also includes the obligation of States to take positive action to eradicate all forms of violence, including manifestations of online violence, even where an individual has not come forward to make a complaint (for example, in the case of online forums generally advocating for violence against women).[40]

(c) Prosecution

68. Prosecution consists in the investigation of and instituting of proceedings against perpetrators. Law enforcement bodies often trivialize online violence against women, and their actions are unfortunately often characterized by a victim-blaming attitude when dealing with these cases. The result of this attitude is a culture of silence and underreporting where women victims are reluctant to speak out for fear of being blamed. Even when women victims succeed in reporting a case and having it investigated, they encounter

[36] See Committee on the Elimination of Discrimination against Women general recommendation No. 35.

[37] See Zarizana Abdul Aziz and Janine Moussa, "Due Diligence Framework: State Accountability for Eliminating Violence against Women", Due Diligence Project, 2014; Zarizana Abdul Azis, "Due Diligence and Accountability for Online Violence against Women", APC Issue Papers, 2017; and Internet Governance Forum, best practice forum on gender access, 2016.

[38] Committee on the Elimination of Discrimination against Women general recommendation No. 35.

[39] See for example the case of *Sabu Mathew George v. Union of India and Others*, Supreme Court of India, 13 December 2017.

[40] See "'Incel': Reddit bans misogynist men's group blaming women for their celibacy", *Guardian*, 8 November 2017.

further obstacles posed by the lack of technical knowledge and ability in the judiciary (including court systems, magistrates and judges). In addition, the costs of litigation prevent many survivors, particularly poorer women, from pursuing their cases in court. It is therefore vital that the responses of first responders — including Internet intermediaries, the police and helplines[41] — and of the judiciary and regulators be assessed in order to achieve a faithful depiction of the reality of women's experiences and to facilitate their access to justice and remedies.

(d) Punishment

69. Punishment entails the duty to punish perpetrators for their crimes by means of sanctions that are necessary and proportionate to the offence. The certainty of adequate punishment conveys the message that ICT-facilitated violence against women and girls will not be tolerated, which is particularly important for women victims of online violence, who often do not receive an effective response from State authorities and perceive a culture of impunity for perpetrators.[42]

(e) Redress, reparation and remedies

70. In most cases, victims of gender-based violence are granted reparations as civil remedies and include financial compensation to cover the costs of the quantifiable losses incurred (such as the cost of medical care, loss of wages and damage to property), injuries and non-quantifiable losses, in addition to the need for survivors to rebuild their lives in the short, medium and long terms. Reparation measures include also the immediate removal of the harmful content as well as forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic, material, individual, and collective, depending on the circumstances and the claims made by the victim. They should also include an immediate injunction to prevent the publication of harmful content.

(f) Role of intermediaries

71. The role of private intermediaries in the regulation and governance of the Internet has progressively come under scrutiny, given that online gender-based violence is usually perpetrated on privately owned platforms, which are frequently in use across many jurisdictions. Internet intermediaries play a central role in providing digital spaces for interaction and, as such, have specific human right responsibilities. These responsibilities have not, however, yet been fully addressed under the international human right framework; for example, while the Guiding Principles on Business and Human Rights affirm the responsibility of business enterprises to respect human rights in general, they do not make any direct reference to the Convention on the Elimination of All Forms of Discrimination against Women or other women's rights instruments (see A/HRC/32/38, para. 37).

72. Internet intermediaries, any corporation storing customers', data, and those providing cloud storage also have the duty to comply with human rights standards by keeping the data secure, and should be accountable for the hacking of data if insufficient safeguards are in place.

73. Although emphasis has been placed on the business and human rights responsibilities of intermediaries, less focus has been placed on how their policies and practices have an impact on women. Research indicates that inadequate and substandard responses from intermediaries concerning online gender-based violence can have a negative effect on freedom of expression, resulting in censorship by platforms, self-censorship or

[41] Digital Rights Foundation, "December 2017: One Year of the Cyber Harassment Helpline Countering Online Violence", 7 January 2018.

[42] See Internet Governance Forum, *Best Practice Forums: Handbook 2015*.

censorship by other users, and do not provide victims of harassment with any form of redress.[43]

74. Many intermediaries have now developed policies that allow for the identification, reporting and rectification of incidents of harassment or violence against women committed on the platforms of Internet service providers. In particular, social media intermediaries have established separate mechanisms to address online abuse, including through the establishment of internal rules aimed at "blocking" online abusers or removing contents that are not considered permissible.

75. Another issue relating to the policies of intermediaries is anonymity and pseudonymity. While anonymity provides a veil for harassers and makes it harder to identify and take action against them, anonymity and pseudonymity are also crucial facets of privacy and freedom of expression for women. Women who have anonymous or pseudonymous online profiles are therefore also adversely affected by the policies on anonymity of certain intermediaries. From a gendered perspective, women should be able to use pseudonyms, which can help them to escape an abusive partner, stalkers, repeat harassers and accounts associated with the sharing of non-consensual pornography.[44] As a result, women, especially women human rights defenders, who choose to remain anonymous on websites like Facebook are often reported by harassers for possessing a "fake" profile. Instead of engaging actions against the harassers, intermediaries sometimes require the women concerned to disclose their identity, which can put them at risk of serious harm. For this reason, the policy has come under severe criticism from civil society groups. Responding to these criticisms, Facebook changed its policy slightly and now requires complainants to provide some amount of proof. In this context, human rights safeguards against arbitrary censorship by intermediaries are crucial.[45]

76. Overall, companies seem unwilling to report how much content is being flagged and removed and under what self-designed criteria. Although some attempts have been made, the transparency of decision-making and in the application of standards to guarantee the prompt reporting of gender-based violence on platforms is limited.[46]

77. While preserving anonymity for users is essential, the identification of perpetrators is necessary if online gender-based violence is to be addressed. Access to justice requires identification processes and the ability to link digital identifiers, such as an IP address, to physical devices and perpetrators by an independent judiciary. A variety of carefully tailored legal tools could facilitate such an identification process.

4. National legal efforts to address online and information and communications technology-facilitated violence against women and girls

78. Some cases of online violence against women have drawn media attention and resulted in important debates on the need for legislative reforms, including the adoption of specific laws; for example, the posting of images of a sexual nature shared online that resulted in the tragic suicide of young girls[47] have prompted a debate on the need for legislative reforms, including the adoption of specific laws.

79. Owing to the pace at which online acts of violence against women can be committed, victims require prompt relief from effective legal protection mechanisms, remedies and redress. In reality, however, many States do not have a holistic legal framework on combating and preventing violence against women, including with regard to specific provisions on online and ICT-facilitated violence against women, and have not

[43] See Rima Athar, "From impunity to justice: Improving corporate policies to end technology-related violence against women", Association for Progressive Communications, 2014.

[44] See Lis Miss Hot Mess, "Facebook's 'real name' policy hurts real people and creates a new digital divide", *Guardian*, 3 June 2015.

[45] See IT for Change, "Technology-mediated Violence against Women in India", January 2017.

[46] See "#ToxicTwitter: Violence and Abuse against Women Online", Amnesty International, March 2018.

[47] For instance, in Canada the suicide of two girls prompted the Government of Canada to adopt, in 2015, Bill C-13 on the non-consensual distribution of intimate images.

acceded to all core human rights treaties. This creates multiple barriers to access to justice for women victims and a sense of impunity for perpetrators.

80. Some States have updated their existing legal frameworks to address online violence against women. The legal instruments most frequently used in this regard are cybercrime laws, criminal laws, laws on domestic violence and violence against women, hate speech laws and laws on data protection and privacy.

81. In some legal contexts, current laws may be sufficiently broad and flexible to be applied to some forms of online violence, but this may not be the case everywhere. Where there is no specialized law, victims are compelled to sue perpetrators through a patchwork of related crimes that may not be adequate; for instance, some victims have brought claims under laws relating to the protection of privacy or to defamation. In cases where gaps in criminal laws exist, victims have attempted to seek recourse through civil means, but this does not adequately address their rights to justice and remedy, and contributes to continuing impunity.

82. In many States, the non-consensual online dissemination of intimate or sexually explicit images of an adult person, even if identifying information is included with the image, is not per se illegal. In States where such acts are not criminalized, prosecutors are limited to charging perpetrators with other crimes, such as stalking, harassment, unlawful surveillance or the dissemination of child pornography. Without criminalization, victims cannot protect their human rights to privacy and dignity. Even where criminal laws specifically criminalize the non-consensual distribution of sexually explicit images, many such laws have shortcomings; for example, many criminal laws require evidence of the intent to cause harm or emotional distress to the victim, which may be difficult to prove, making convictions harder to achieve. Moreover, many laws currently in place do not address threats to release a certain image or video.

83. Some States have enacted specific laws to address online stalking, online harassment and the non-consensual sharing of intimate images, while others have applied other domestic laws to address these crimes. There is an example of a State classifying the non-consensual dissemination of sexual images as an aggravating circumstance in domestic violence-related offences, which allowed for penalties for convictions on charges of domestic assault, stalking or violations of a restraining order. Other States have developed legislation on ICT-related offences, such as the unauthorized modification of or access to data and communications.

84. Other States have also expanded the application of family violence protection orders issued by courts to cases of non-consensual distribution of intimate images and cyberstalking. In other cases, victims subjected to online bullying have been given the opportunity to request the court to issue a protection order against an individual. Some States also require electronic service providers to assist courts in the identification of individuals responsible for cyberbullying, which allows victims to sue perpetrators for damages.

85. Even when a specialized legal framework is in place, legal and regulatory mechanisms, including law enforcement officials, are not always trained or equipped to implement it effectively owing to the lack of adequate gender-sensitive training and the general perception that online abuse is not a serious crime.

5. Civil society-led initiatives

86. Certain non-governmental organization-led initiatives, such as specialized helplines, have been organized with a view to providing support to women and girls who have been subjected to online gender-based violence. One example is the Access Now Digital Security Helpline,[48] which helps women at risk to improve their digital security practices and provides rapid-response emergency assistance for women already under attack. The service, which is available 24 hours a day, seven days a week in eight languages, aims to respond to all requests it receives within two hours. Another example is the Digital Rights

[48] See www.accessnow.org/help/.

Foundation,[49] based in Pakistan, which addresses online harassment, technology and gender through research, advocacy and service delivery. Its Cyber Harassment Helpline is the region's first dedicated helpline for cases of online harassment and violence.

87. Awareness-raising initiatives have been organized, such as the Internet Democracy Project,[50] a not-for-profit initiative based in New Delhi, which provides research, advocacy and spaces for debate on online violence and its prevention. In Germany, rape crisis centres and women's counselling centres seek to raise awareness, provide support and educate on preventing online violence.[51] Another example is the International Federation of Journalists, which, together with the South Asia Media Solidarity Network, has campaigned against the online abuse of women journalists and launched in March 2017 the ByteBack campaign, dedicated to fighting online harassment.[52] The Association for Progressive Communications, a global network of non-governmental organizations, has organized the "End violence: Women's rights and safety online" project, which focuses on capacity-building for human rights activists and women's organizations in the use of technology in their activities.

88. Lastly (among many others), the Project Shift: Creating a Safer Digital World for Young Women, led by YWCA Canada, aims to prevent and eliminate cyberviolence against young women and girls. The project has also led to the preparation of "A Guide for Trusted Adults: Practical Tips and Tools for Supporting Girls and Young Women Navigating Life Online".[53]

IV. Conclusion and recommendations

89. **International human rights law and the Sustainable Development Goals and targets on achieving gender equality, empowering women and girls and eliminating violence against women in public and private life are fully applicable in digital spaces and actions enabled by ICT. Moreover, the principle that human rights and women's rights protected offline must also be protected online should fully integrate the right to live free from emerging forms of online and ICT-facilitated violence against women, while respecting the right to freedom of expression and the right to privacy and data protection. Given its characteristics, ICT should serve as a tool for accelerating the achievement of all human rights, including gender equality, the empowerment of women and the elimination of discrimination and violence against women.**

90. **Legal and policy measures to eradicate online gender-based violence against women should be framed within the broader framework of human rights that addresses the structural discrimination, violence and inequalities that women face, and seek to create an enabling environment for achieving gender equality through the use of ICT.**

91. **To achieve the above-mentioned goals, any effective response to online gender-based violence against women will require the cooperation of States, Internet intermediaries and all other stakeholders on the acceptance and implementation of all core international human rights instruments, including those on women's rights.**

A. Recommendations for the United Nations

92. **The Special Rapporteur on the right to privacy, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on violence against women, its causes and consequences, and other special procedure mandate holders and relevant treaty bodies should**

[49] See https://digitalrightsfoundation.pk/cyber-harassment-helpline.
[50] See http://internetdemocracy.in.
[51] See www.frauen-gegen-gewalt.de/the-federal-association.html.
[52] See https://samsn.ifj.org/ifj-byteback-campaign/.
[53] Available from http://ywcacanada.ca/data/documents/00000543.pdf.

coordinate, with the support of OHCHR and UN-Women, to tackle human right violations online, in general, and online violence against women, in particular, in their work, reports and recommendations.

B. Recommendations for States

93. States should recognize online and ICT-facilitated violence against women as a human rights violation and a form of discrimination and gender-based violence against women, and duly apply core international human rights instruments.

94. States should implement the principle that the human rights and women's rights protected offline should be protected online by the ratification and implementation of all core human rights treaties.

95. States should, in accordance with the principle of due diligence, enact new laws and measures to prohibit new emerging forms of online gender-based violence. Such laws should be grounded in international women's human rights law and standards, as outlined in the Convention on the Elimination of All Forms of Discrimination against Women (with due consideration for general recommendations Nos. 19 and 35 of the Committee on the Elimination of Discrimination against Women) and the Declaration on the Elimination of Violence against Women, and in other global and regional women's human rights instrument, such as the Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Belém do Pará Convention), the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa. Furthermore, States should ensure that their legal frameworks adequately protect all women's human rights online, including the right to life free from violence, freedom of expression and access to information, and the right to privacy and data protection.

96. States should collect and publish data disaggregated by sex on Internet and ICT availability, and take measures to eliminate any gender inequality in access to technologies, in accordance with article 4.1 of the Convention on the Elimination of All Forms of Discrimination against Women.

97. States should also promote digital literacy in the use of the Internet and ICT for all, without sex- or gender-based discrimination, and promote gender equality at all levels of education, including online education, from early childhood onwards.

98. States should draft a United Nations resolution on women's human rights and online and ICT-facilitated violence against women, and develop United Nations guidelines on the role of intermediaries in that respect.

99. States should, in accordance with the principle of due diligence, ensure that regulations on Internet intermediaries respect the international human rights framework, including that with regard to business and human rights, which should be explicitly expanded to include women's human rights instruments that prohibit gender-based violence online.

100. States should ensure that effective measures are taken to prevent the publication of harmful material that comprises gender-based violence against women, and for their removal on an urgent basis. States should adopt, or adapt (as appropriate) their criminal and civil causes of action to hold perpetrators liable. Such legislative measures should be applicable also to threats of releasing harmful information or content online.

101. States should clearly prohibit and criminalize online violence against women, in particular the non-consensual distribution of intimate images, online harassment and stalking. The criminalization of online violence against women should encompass all elements of this type of abuse, including subsequent "re-sharing" of harmful content. The threat to disseminate non-consensual images must be made illegal so that

advocates and prosecutors may intervene and prevent the abuse before it is perpetrated.

102. **States should apply a gender perspective to all online forms of violence, which are usually criminalized in a gender-neutral manner, in order to address them as acts of gender-based violence. Criminal or civil causes of action should allow women victims to pursue legal action, with adequate protection of their privacy, and avoid secondary victimization of women; without such protection, victims attempting to erase content may be exposed to the risk of having their case made even more public.**

103. **States should provide victims with legal recourse and appropriate legal aid in order that they may request from the court an order that harmful content be destroyed, in addition to an interim order that the perpetrator promptly cease circulating the material pending a resolution of the legal case, in collaboration with Internet intermediaries.**

104. **States should allow victims to obtain protection orders (for example, restraining orders) in family or civil courts to prevent their abusers from posting or sharing intimate images without their consent or engaging in other form of harassment or violence, whether online or offline.**

105. **States should provide training for magistrates, lawyers, police and all other law enforcement officials and frontline workers to ensure their ability to investigate and prosecute perpetrators, and foster public trust in obtaining justice for cases of online and ICT-facilitated violence.**

106. **States should also develop specialized, clear, efficient and transparent internal and external protocols and codes of conduct for its law enforcement officials addressing online violence against women to enable them to better understand that online violence is a form of gender-based violence that warrants a serious, trauma-informed response.**

107. **States should provide protective measures and services for victims of online gender-based violence: this includes specialized helplines to provide support to those who have been attacked online, shelters and protection orders.**

108. **States should provide reparation measures, which should not, however, rely on compensation only. Such measures should include forms of restitution, rehabilitation, satisfaction and guarantees of non-repetition, combining measures that are symbolic, material, individual and collective, depending on the circumstances and the preferences of the victim.**

109. **States should develop their cooperation with private intermediaries and national human rights institutions, and support civil society organizations that address online violence against women.**

110. **States should provide education, outreach and gender-sensitive training for Internet users on online and ICT-facilitated violence against women and girls in schools and communities as a way to prevent it.**

111. **States should inform children and teenagers about the risks of taking, or allowing others to take, intimate images, and that the dissemination of such images is a form of gender-based violence and a crime. Girls should also learn about safety on social media platforms and the Internet, and how to protect their own privacy online.**

112. **States should guarantee the enforcement of strong data protection regulations and ensure the accountability of data holders in cases of breach.**

113. **States should protect and encourage the development of technology, including of encryption and anonymity tools that protect the rights and security of women online.**

114. **States should periodically publish incident reports at the national level, in cooperation with private intermediaries, and promote the creation of national observatories of online and ICT-facilitated violence against women and girls.**

C. Recommendations for Internet intermediaries

115. **Internet intermediaries should uphold the principle that human rights are protected online, and voluntary accept and apply all core international human rights and women's rights instruments with a view to contributing to universal human rights protection and achieving the empowerment of women, and the elimination of discrimination and violence against them in digital space. In this respect, they should actively cooperate with the treaty bodies and the special procedures, and in particular with the Special Rapporteur on violence against women, its causes and consequences, and with independent international and regional women's rights mechanisms.**

116. **Intermediaries should adopt transparent complaint mechanisms for cases of online and ICT-facilitated violence against women and girls. Policies and procedures for reporting and requesting the removal of harmful content should be easily accessible and transparent. Intermediaries should publish clear and a comprehensive contents moderation policy and human rights safeguards against arbitrary censorship, and transparent reviews and appeal processes.**

117. **Intermediaries should provide terms of service and reporting tools in local languages. Reporting tools should be accessible, user-friendly and easy to find.**

118. **Intermediaries should ensure data security and privacy, and ensure that the use of data is in compliance with international human rights law and has the fully informed consent of data providers.**

119. **Internet platforms should commit to eradicating online gender-based violence. In this sense, they should allocate resources to information and education campaigns on preventing ICT-facilitated violence against women and girls and on promoting human rights and digital security.**